

# FortiGate on Microsoft Azure

Gabriel Kälin, Fortinet

October 24, 2018

# Agenda

- Scenario 1: Single FortiGate on Azure for IPsec VPN to on-premise
  - » Using the FortiGate to Azure Connector
  - » Automation with template deployment
- Scenario 2: HA Active-Passive
- Scenario 3: Network Segmentation
- Scenario 4: Cloud DMZ with HA Active-Active



# Scenario 1: Single FortiGate on Azure for IPsec VPN to on-premise

# Azure Marketplace

Microsoft Azure

Why Azure Solutions Products Documentation Pricing Training Marketplace Partners Blog Resources Support

FREE ACCOUNT >

Azure Marketplace

Browse Sell Learn

Search Marketplace

Sign in

Product Category

Compute Networking Storage Web + Mobile Databases Intelligence + analytics Security + Identity Developer tools Monitoring + Management Add-ons Blockchain Azure Active Directory apps

Refine

Trial

☐ Test Drive ☐ Free software trial

Pricing Model

☐ Free ☐ Pay as you go ☐ Bring your own license (BYO)

Operating System


☐ Windows ☐ Linux

Publisher

☐ Partners ☐ Microsoft

Fortinet

Product results (6)




Fortinet FortiWeb Web Application Firewall (WAF)

By Fortinet

FortiWeb Web Application Firewall delivers multi-layered application threat protection

Price varies

Test Drive




FortiGate Next Generation Firewall for HA

By Fortinet

High Availability Azure Resource Manager Template for FortiGate Next Generation Firewall

Price varies

Test Drive




FortiAnalyzer Centralized Log Analytics

By Fortinet

Fortinet FortiAnalyzer delivers centralized network logging, analytics, and reporting

Price varies

Get it now



FortiManager Centralized Security Management


By Fortinet

Reduce costs, simplify configuration, automate provisioning & maintain compliance with FortiManager

Price varies

Get it now

Products > FortiGate Next Generation Firewall for HA



FortiGate Next Generation Firewall for HA

Fortinet

Overview Plans

GET IT NOW

TEST DRIVE

What's Test Drive?

Test Drive duration 1 hour

Pricing information Cost of deployed template components

Categories Compute Networking Security + Identity

Legal License Agreement Privacy Policy

Software plan

FortiGate NGFW High Availability (HA)

Description

Fortinet FortiGate Next Generation Firewall complements the base security on Microsoft Azure platform. As you start the ARM template deployment, you will be guided to select either **Bring Your Own License or Pay as You Go hourly licensing** selection.

FortiGate Bring-Your-Own-License (BYOL) option allows you to pick and choose the VM annual perpetual licenses with various vCPU configuration.

This template provides a base start for HA architecture required for Enterprise environments. Configured to include the components and settings to deliver best in class security with the HA protection needed for today's mission critical workloads.

- FortiGate VM offers protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating system.
- IPS technology protects against network-level threats in addition to signature-based threat detection, IPS performs anomaly-based detection which alerts users to any traffic that matches attack behavior profiles.

For technical support assistance, you will need to register the FortiGate-VM license for Azure at the Fortinet Customer Support <https://support.fortinet.com/>.

In addition to PAYG and BYOL licensing options, you can start your trial license directly from your Azure portal or obtain an evaluation license for BYOL from your sales representative or channel partner.

Azure Pay-As-You-Go pricing reference

CPU	Azure Instances Supported	FortiGate License Cost*
1 vCPU	D1_v2, F1, F1s;	\$0.30/hr
2 vCPU;	D2_v2, F2, F2s;	\$0.73/hr
4 vCPU;	D3_v2, F4, F4s	\$0.98/hr
8 vCPU;	D4_v2, F8, F8s;	\$1.96/hr

\*Price is added to compute charges

FORTINET

4

# How to Choose the Right FortiGate Model

- Use v-Series FortiGate VM: FG-VMxxV
  - » VDOM use restricted by number of NICs.
  - » VDOM upgrade possible
  - » Management VDOM will be available by default
- New with FortiOS 6.0.2 and later: FortiGate VM can run on larger instances w.r.t. vCPU than the license would allow. Excess vCPUs will be ignored.

Instance type	vCPU	Max NIC	FortiGate minimum order (BYOL)
F1	1	2	FG-VM01 or FG-VM01v
F2, F2s, F2s_v2	2	2	FG-VM02 or FG-VM02v
F4, F4s, F4s_v2	4	4 (2 for F4s_v2)	FG-VM04 or FG-VM04v
F8, F8s, F8s_v2	8	8 (4 for F8s_v2)	FG-VM08 or FG-VM08v
F16, F16s, F16s_v2	16	8 (4 for F16s_v2)	FG-VM16 or FG-VM16v

<https://docs2.fortinet.com/vm/azure/fortigate/6.0/about-fortigate-for-azure/6.0.0/271726/instance-type-support>

# Custom Sample Templates from Fortinet

Features Business Explore Marketplace Pricing Search GitHub Sign in or Sign up

Overview Repositories 2 Stars 0 Followers 21 Following 6

**Fortinet Solutions**  
fortinetsolutions

Security Without Compromise

Block or report user

Fortinet, Inc.  
Sunnyvale, California  
<https://www.fortinet.com/>

**Popular repositories**

- [Azure-Templates](#)  
Azure Templates for Fortinet Solutions  
★ 6 🍴 5
- [AWS-CloudFormationTemplates](#)  
AWS Cloud Formation Templates for Fortinet Solutions  
HCL ★ 4

8 contributions in the last year

Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct

Mon  
Wed  
Fri

[Learn how we count contributions.](#)

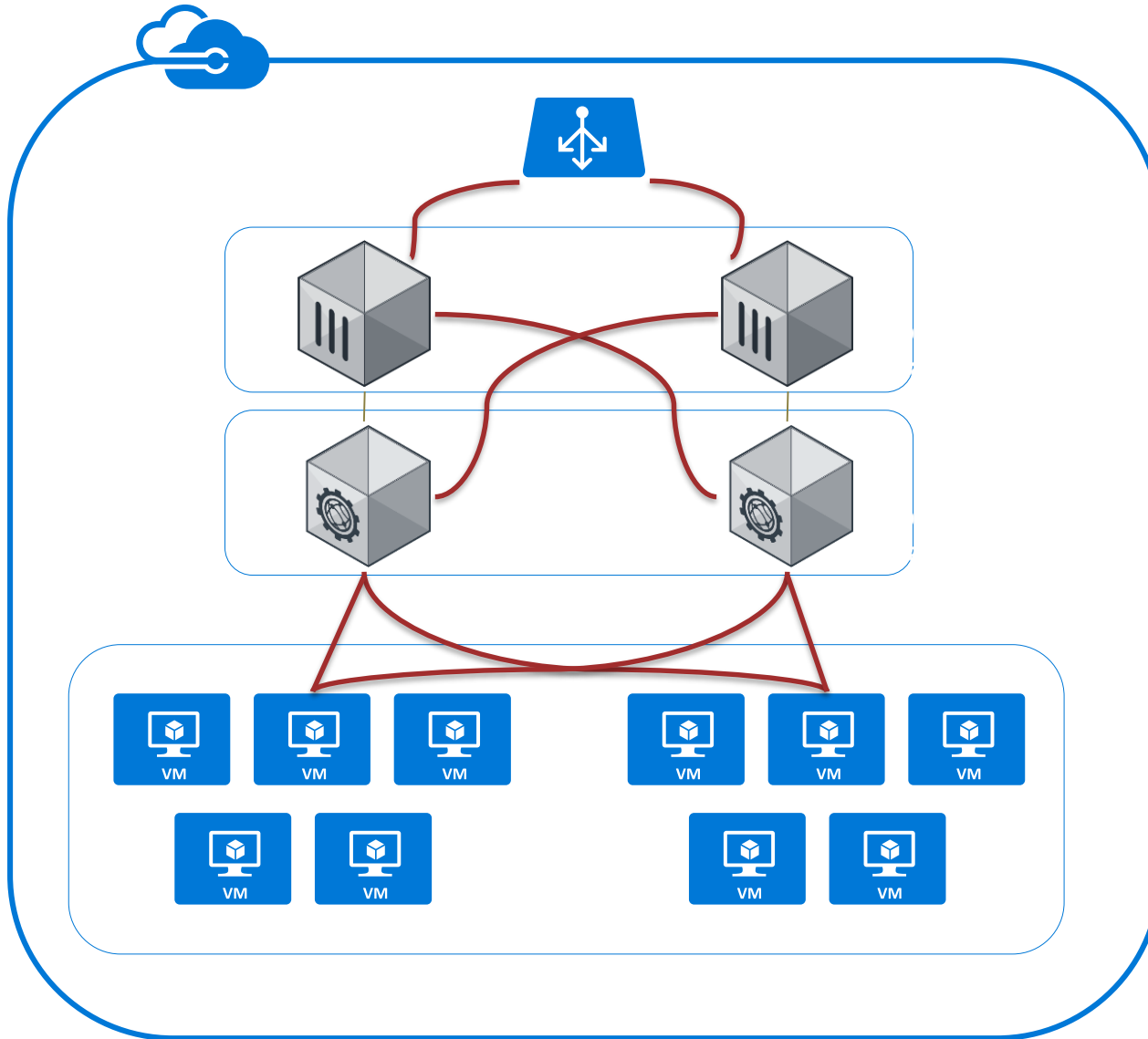
Less More

Contribution activity Jump to 2017

<https://github.com/fortinetsolutions>



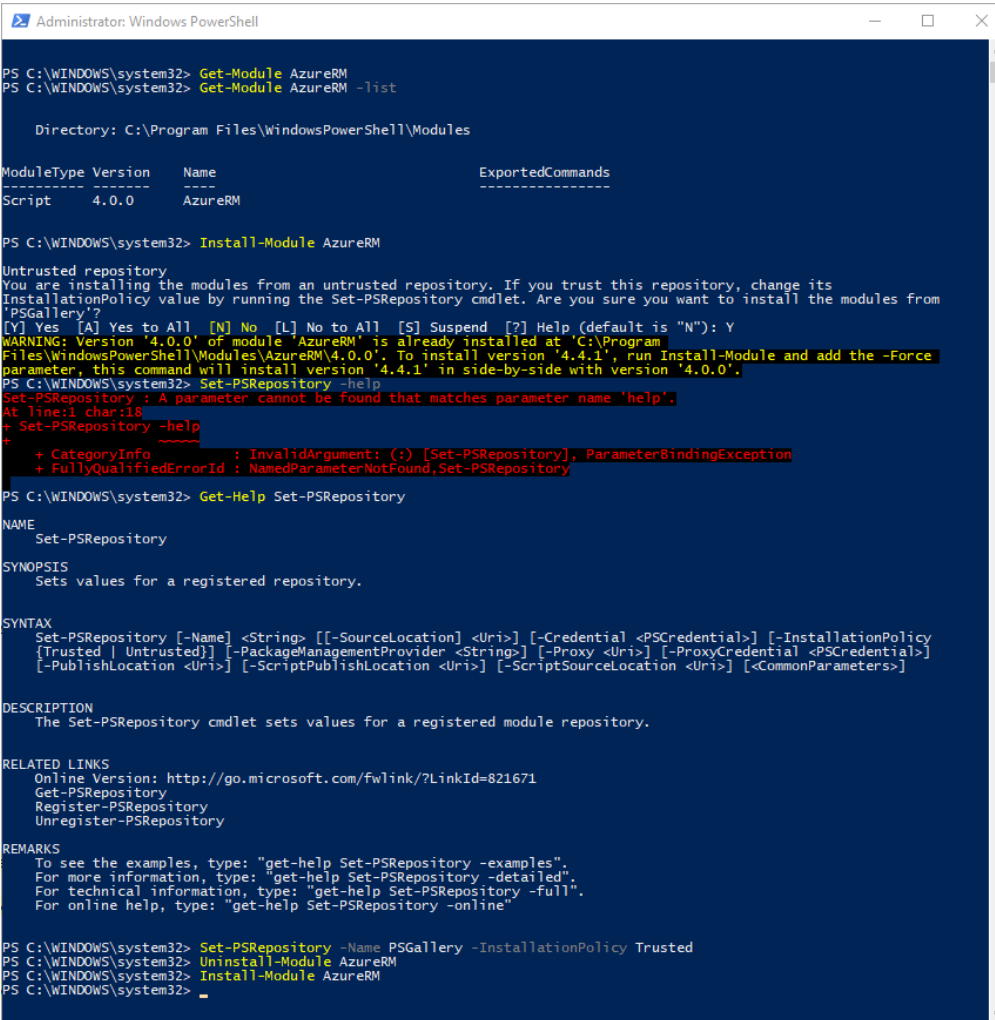
# FortiGate on Azure – Living with playground rules



1. You may not manipulate layer 2
2. You may not use Multicast
3. You may not reassign IP addresses
4. You may create one and only one next hop per custom route.

# Azure with PowerShell – Getting Started

- If you're starting with PowerShell (PS):
  - » Trust the repository "PSGallery" to avoid warnings
    - Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
  - » Allow execution of local scripts, e.g.
    - Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy remotesigned
- Install Azure Resource Manager module
  - » Get-Module AzureRM
  - » Import-Module AzureRM
- Check installed version of AzureRM
  - » Get-Module AzureRM -ListAvailable
- If there is a new version available
  - » Update-Module AzureRM



```
Administrator: Windows PowerShell

PS C:\WINDOWS\system32> Get-Module AzureRM
PS C:\WINDOWS\system32> Get-Module AzureRM -list

Directory: C:\Program Files\WindowsPowerShell\Modules

ModuleType Version Name ExportedCommands
-----
Script 4.0.0 AzureRM

PS C:\WINDOWS\system32> Install-Module AzureRM

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
WARNING: Version '4.0.0' of module 'AzureRM' is already installed at 'C:\Program
Files\WindowsPowerShell\Modules\AzureRM\4.0.0'. To install version '4.4.1', run Install-Module and add the -Force
parameter, this command will install version '4.4.1' in side-by-side with version '4.0.0'.
PS C:\WINDOWS\system32> Set-PSRepository -help
Set-PSRepository: A parameter cannot be found that matches parameter name 'help'.
At line:1 char:18
+ Set-PSRepository -help
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Set-PSRepository], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Set-PSRepository

PS C:\WINDOWS\system32> Get-Help Set-PSRepository

NAME
Set-PSRepository

SYNOPSIS
Sets values for a registered repository.

SYNTAX
Set-PSRepository [-Name] <String> [[-SourceLocation] <Uri>] [-Credential <PSCredential>] [-InstallationPolicy
{Trusted | Untrusted}] [-PackageManagementProvider <String>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-PublishLocation <Uri>] [-ScriptPublishLocation <Uri>] [-ScriptSourceLocation <Uri>] [<CommonParameters>]

DESCRIPTION
The Set-PSRepository cmdlet sets values for a registered module repository.

RELATED LINKS
Online Version: http://go.microsoft.com/fwlink/?LinkId=821671
Get-PSRepository
Register-PSRepository
Unregister-PSRepository

REMARKS
To see the examples, type: "get-help Set-PSRepository -examples".
For more information, type: "get-help Set-PSRepository -detailed".
For technical information, type: "get-help Set-PSRepository -full".
For online help, type: "get-help Set-PSRepository -online"

PS C:\WINDOWS\system32> Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
PS C:\WINDOWS\system32> Uninstall-Module AzureRM
PS C:\WINDOWS\system32> Install-Module AzureRM
PS C:\WINDOWS\system32>
```




# Using Azure Connectors

# Security Fabric connector for Azure






- Part of FortiOS 6.0 multi-cloud Security Fabric support
- Also to update dynamic addresses

Edit Address

Name	HAtestUbuntu
Color	 <input type="button" value="Change"/>
Type	Fabric Connector Address ▾
Fabric Connector Type	Microsoft Azure ▾
Filter	vm=HAtestUbuntu
Interface	<input type="checkbox"/> any ▾
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text"/> 0/255

Tags

## Edit Fabric Connector

Name	azure
Type 	<div>Application Centric Infrastructure (ACI)</div> <div>Amazon Web Services (AWS)</div> <div><b>Microsoft Azure</b></div> <div>VMware NSX</div> <div>Nuage Virtualized Services Platform</div>
Azure tenant ID 	9cbc2019-cdee-4834-9258-41c500341
Azure client ID 	fd6cef6e-76d4-46df-b151-7721b75bf7
Azure client secret 	..... <input type="button" value="Change"/>
Azure subscription ID	4ea46438-80d3-4abe-ad07-e28a9631
Azure resource group	NewHARG
Update Interval 	<input checked="" type="button" value="Use Default"/> <input type="button" value="Specify"/>
Status	<input checked="" type="checkbox"/>

# Azure SDN Connector supported filters

- set filter 'vm=<name>'
  - set filter 'securitygroup=<nsg name>'
  - set filter 'vnet=<virtual network name>'
  - set filter 'subnet=<subnet name>'
  - set filter 'vmss=<vmss name>'
  - set filter 'tag.<key>=<value>'
  - set filter 'vm=<name> & vnet=<virtual network name>'
  - set filter 'vm=<name> | vm=<name>'
- 
- Current implementation will limit the use to one Azure subscription, and only resources in use and associated with running VMs
  - FortiOS 6.2 will enable multiple connectors of the same type

# License and Config Bootstrapping

Deployment with custom data in Template with PowerShell

# How to Format Custom Data

- Requires base64 encoded multipart/mixed content
- Use/insert customData attribute in osProfile section of template.json

## Example

```
Content-Type: multipart/mixed; boundary="=====0086047718136476635=="
MIME-Version: 1.0
```

```
-----0086047718136476635==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"
```

```
config sys global
    set admintimeout 120
    set hostname "mycloudinit"
    set timezone 26
end
```

```
-----0086047718136476635==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="FGVM010000156211.lic"
```

```
-----BEGIN FGT VM LICENSE-----
QAAAAOckKptgXQ0Mvc/3UNfiIqGohp8MGWOCWh+wSqzcfQV/7e5suEXkls5Uvm9b
ww/aX3dxCvp0FVRTDmadfdbHwFgAAAAC+a0I1JRT+b72wqY+jUzH7/AW4I1AhIU
f4EPIKgrKoFxdIazYhBXTYw0UeokRx0ySNqM1YzfdWEa26Gq9/ecdt1FKYKeJ21f
ptbePSNd2w8emQbk5yvlm4i3npJT+YgO
-----END FGT VM LICENSE-----
```

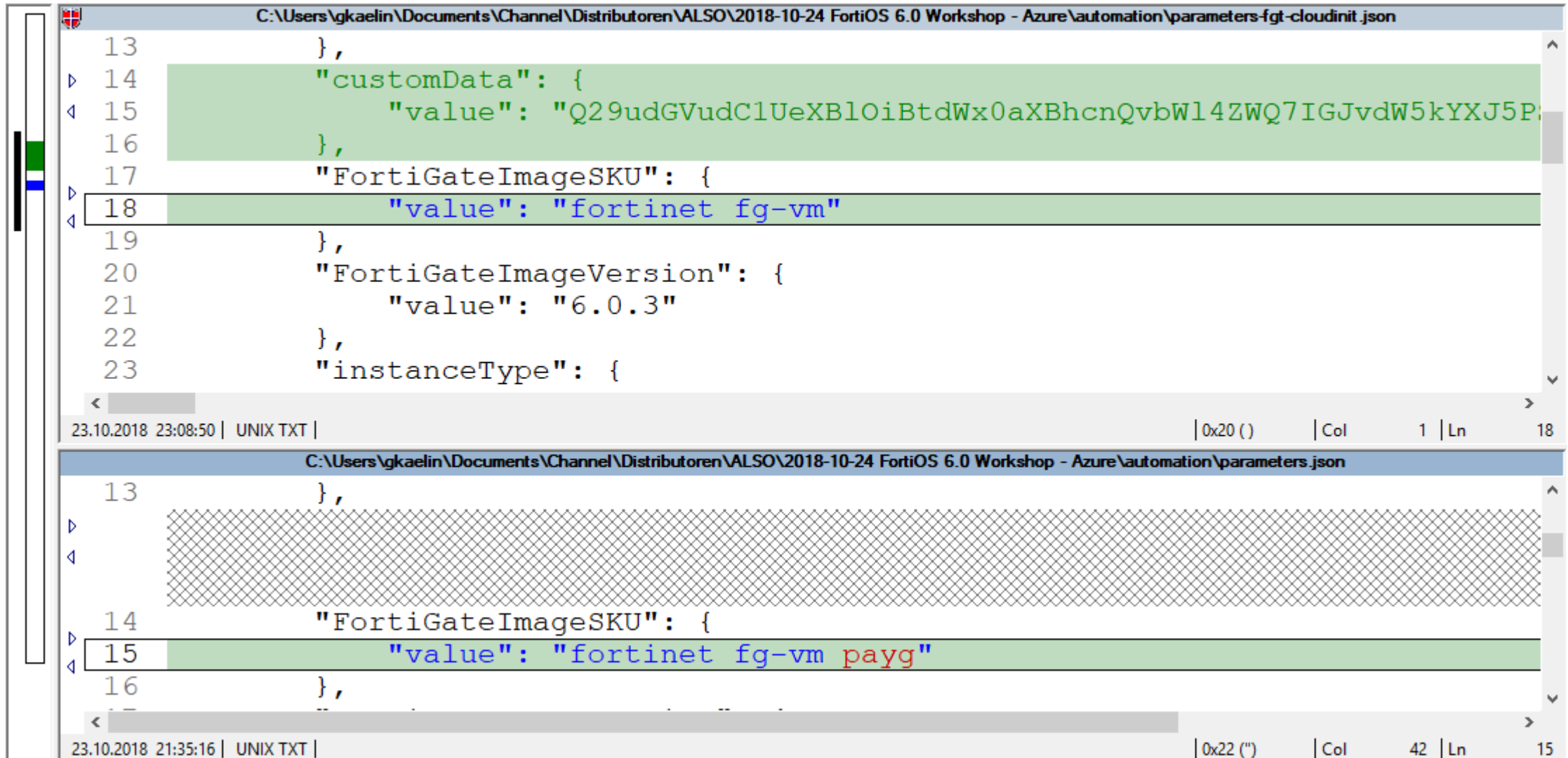
```
-----0086047718136476635----
```

# Insert customData Field Into Template

```
C:\Users\gkaelin\Documents\Channel\Distributoren\ALSO\2018-10-24 FortiOS 6.0 Workshop - Azure\automation\preparation\template-fgt-cloudinit.json
20      "description": "Password for the FortiGate virtual appliance."
21    }
22  },
23  "customData": {
24    "type": "string",
25    "metadata": {
26      "description": "check Mantis 0449239 for data format"
27    }
28  },
29  "FortiGateName": {
30    "type": "string",
31    "metadata": {
32      "description": "Name for FortiGate virtual appliance."
33    }
34  },
35  "id": "[variables('compute_AvailabilitySet_FG_Id')]",
36  },
37  "osProfile": {
38    "computerName": "[parameters('FortiGateName')]",
39    "adminUsername": "[parameters('adminUsername')]",
40    "adminPassword": "[parameters('adminPassword')]",
41    "customData": "[parameters('customData')]"
42  },
43  "storageProfile": {
44    "id": "[variables('compute_AvailabilitySet_FG_Id')]",
45    },
46    "osProfile": {
47      "computerName": "[parameters('FortiGateName')]",
48      "adminUsername": "[parameters('adminUsername')]",
49      "adminPassword": "[parameters('adminPassword')]",
50      "customData": "[parameters('customData')]"
51    },
52    "storageProfile": {
53      "imageReference": {
54        "publisher": "MicrosoftWindowsServer",
55        "offer": "WindowsServer",
56        "sku": "2016-Datacenter",
57        "skuinc": "2016-Datacenter",
58        "version": "2016.09",
59        "arch": "x64"
60      }
61    }
62  }
63  },
64  "storageProfile": {
65    "id": "[variables('compute_AvailabilitySet_FG_Id')]",
66    },
67    "osProfile": {
68      "computerName": "[parameters('FortiGateName')]",
69      "adminUsername": "[parameters('adminUsername')]",
70      "adminPassword": "[parameters('adminPassword')]",
71      "customData": "[parameters('customData')]"
72    },
73    "storageProfile": {
74      "imageReference": {
75        "publisher": "MicrosoftWindowsServer",
76        "offer": "WindowsServer",
77        "sku": "2016-Datacenter",
78        "skuinc": "2016-Datacenter",
79        "version": "2016.09",
80        "arch": "x64"
81      }
82    }
83  }
84  },
85  "storageProfile": {
86    "id": "[variables('compute_AvailabilitySet_FG_Id')]",
87    },
88    "osProfile": {
89      "computerName": "[parameters('FortiGateName')]",
90      "adminUsername": "[parameters('adminUsername')]",
91      "adminPassword": "[parameters('adminPassword')]",
92      "customData": "[parameters('customData')]"
93    },
94    "storageProfile": {
95      "imageReference": {
96        "publisher": "MicrosoftWindowsServer",
97        "offer": "WindowsServer",
98        "sku": "2016-Datacenter",
99        "skuinc": "2016-Datacenter",
100       "version": "2016.09",
101       "arch": "x64"
102     }
103   }
104 }
105 }
106 }
107 }
108 }
109 }
110 }
111 }
112 }
113 }
114 }
115 }
116 }
117 }
118 }
119 }
120 }
121 }
122 }
123 }
124 }
125 }
126 }
127 }
128 }
129 }
130 }
131 }
132 }
133 }
134 }
135 }
136 }
137 }
138 }
139 }
140 }
141 }
142 }
143 }
144 }
145 }
146 }
147 }
148 }
149 }
150 }
151 }
152 }
153 }
154 }
155 }
156 }
157 }
158 }
159 }
160 }
161 }
162 }
163 }
164 }
165 }
166 }
167 }
168 }
169 }
170 }
171 }
172 }
173 }
174 }
175 }
176 }
177 }
178 }
179 }
180 }
181 }
182 }
183 }
184 }
185 }
186 }
187 }
188 }
189 }
190 }
191 }
192 }
193 }
194 }
195 }
196 }
197 }
198 }
199 }
200 }
201 }
202 }
203 }
204 }
205 }
206 }
207 }
208 }
209 }
210 }
211 }
212 }
213 }
214 }
215 }
216 }
217 }
218 }
219 }
220 }
221 }
222 }
223 }
224 }
225 }
226 }
227 }
228 }
229 }
230 }
231 }
232 }
233 }
234 }
235 }
236 }
237 }
238 }
239 }
240 }
241 }
242 }
243 }
244 }
245 }
246 }
247 }
248 }
249 }
250 }
251 }
252 }
253 }
254 }
255 }
256 }
257 }
258 }
259 }
260 }
261 }
262 }
263 }
264 }
265 }
266 }
267 }
268 }
269 }
270 }
271 }
272 }
273 }
274 }
275 }
276 }
277 }
278 }
279 }
280 }
281 }
282 }
283 }
284 }
285 }
286 }
287 }
288 }
289 }
290 }
291 }
292 }
293 }
294 }
295 }
296 }
297 }
298 }
299 }
300 }
301 }
302 }
303 }
304 }
305 }
306 }
307 }
308 }
309 }
310 }
311 }
312 }
313 }
314 }
315 }
316 }
317 }
318 }
319 }
320 }
321 }
322 }
323 }
324 }
325 }
326 }
327 }
328 }
329 }
330 }
331 }
332 }
333 }
334 }
335 }
336 }
337 }
338 }
339 }
340 }
341 }
342 }
343 }
344 }
345 }
346 }
347 }
348 }
349 }
350 }
351 }
352 }
353 }
354 }
355 }
356 }
357 }
358 }
359 }
360 }
361 }
362 }
363 }
364 }
365 }
366 }
367 }
368 }
369 }
370 }
371 }
372 }
373 }
374 }
375 }
376 }
377 }
378 }
379 }
380 }
381 }
382 }
383 }
384 }
385 }
386 }
387 }
388 }
389 }
390 }
391 }
392 }
393 }
394 }
395 }
396 }
397 }
398 }
399 }
400 }
401 }
402 }
403 }
404 }
405 }
406 }
407 }
408 }
409 }
410 }
411 }
412 }
413 }
414 }
415 }
416 }
417 }
418 }
419 }
420 }
421 }
422 }
423 }
424 }
425 }
426 }
427 }
428 }
429 }
430 }
431 }
432 }
433 }
434 }
435 }
436 }
437 }
438 }
439 }
440 }
441 }
442 }
443 }
444 }
445 }
446 }
447 }
448 }
449 }
450 }
451 }
452 }
453 }
454 }
455 }
456 }
457 }
458 }
459 }
460 }
461 }
462 }
463 }
464 }
465 }
466 }
467 }
468 }
469 }
470 }
471 }
472 }
473 }
474 }
475 }
476 }
477 }
478 }
479 }
480 }
481 }
482 }
483 }
484 }
485 }
486 }
487 }
488 }
489 }
490 }
491 }
492 }
493 }
494 }
495 }
496 }
497 }
498 }
499 }
500 }
501 }
502 }
503 }
504 }
505 }
506 }
507 }
508 }
509 }
510 }
511 }
512 }
513 }
514 }
515 }
516 }
517 }
518 }
519 }
520 }
521 }
522 }
523 }
524 }
525 }
526 }
527 }
528 }
529 }
530 }
531 }
532 }
533 }
534 }
535 }
536 }
537 }
538 }
539 }
540 }
541 }
542 }
543 }
544 }
545 }
546 }
547 }
548 }
549 }
550 }
551 }
552 }
553 }
554 }
555 }
556 }
557 }
558 }
559 }
560 }
561 }
562 }
563 }
564 }
565 }
566 }
567 }
568 }
569 }
570 }
571 }
572 }
573 }
574 }
575 }
576 }
577 }
578 }
579 }
580 }
581 }
582 }
583 }
584 }
585 }
586 }
587 }
588 }
589 }
590 }
591 }
592 }
593 }
594 }
595 }
596 }
597 }
598 }
599 }
600 }
601 }
602 }
603 }
604 }
605 }
606 }
607 }
608 }
609 }
610 }
611 }
612 }
613 }
614 }
615 }
616 }
617 }
618 }
619 }
620 }
621 }
622 }
623 }
624 }
625 }
626 }
627 }
628 }
629 }
630 }
631 }
632 }
633 }
634 }
635 }
636 }
637 }
638 }
639 }
640 }
641 }
642 }
643 }
644 }
645 }
646 }
647 }
648 }
649 }
650 }
651 }
652 }
653 }
654 }
655 }
656 }
657 }
658 }
659 }
660 }
661 }
662 }
663 }
664 }
665 }
666 }
667 }
668 }
669 }
670 }
671 }
672 }
673 }
674 }
675 }
676 }
677 }
678 }
679 }
680 }
681 }
682 }
683 }
684 }
685 }
686 }
687 }
688 }
689 }
690 }
691 }
692 }
693 }
694 }
695 }
696 }
697 }
698 }
699 }
700 }
701 }
702 }
703 }
704 }
705 }
706 }
707 }
708 }
709 }
710 }
711 }
712 }
713 }
714 }
715 }
716 }
717 }
718 }
719 }
720 }
721 }
722 }
723 }
724 }
725 }
726 }
727 }
728 }
729 }
730 }
731 }
732 }
733 }
734 }
735 }
736 }
737 }
738 }
739 }
740 }
741 }
742 }
743 }
744 }
745 }
746 }
747 }
748 }
749 }
750 }
751 }
752 }
753 }
754 }
755 }
756 }
757 }
758 }
759 }
760 }
761 }
762 }
763 }
764 }
765 }
766 }
767 }
768 }
769 }
770 }
771 }
772 }
773 }
774 }
775 }
776 }
777 }
778 }
779 }
780 }
781 }
782 }
783 }
784 }
785 }
786 }
787 }
788 }
789 }
790 }
791 }
792 }
793 }
794 }
795 }
796 }
797 }
798 }
799 }
800 }
801 }
802 }
803 }
804 }
805 }
806 }
807 }
808 }
809 }
810 }
811 }
812 }
813 }
814 }
815 }
816 }
817 }
818 }
819 }
820 }
821 }
822 }
823 }
824 }
825 }
826 }
827 }
828 }
829 }
830 }
831 }
832 }
833 }
834 }
835 }
836 }
837 }
838 }
839 }
840 }
841 }
842 }
843 }
844 }
845 }
846 }
847 }
848 }
849 }
850 }
851 }
852 }
853 }
854 }
855 }
856 }
857 }
858 }
859 }
860 }
861 }
862 }
863 }
864 }
865 }
866 }
867 }
868 }
869 }
870 }
871 }
872 }
873 }
874 }
875 }
876 }
877 }
878 }
879 }
880 }
881 }
882 }
883 }
884 }
885 }
886 }
887 }
888 }
889 }
890 }
891 }
892 }
893 }
894 }
895 }
896 }
897 }
898 }
899 }
900 }
901 }
902 }
903 }
904 }
905 }
906 }
907 }
908 }
909 }
910 }
911 }
912 }
913 }
914 }
915 }
916 }
917 }
918 }
919 }
920 }
921 }
922 }
923 }
924 }
925 }
926 }
927 }
928 }
929 }
930 }
931 }
932 }
933 }
934 }
935 }
936 }
937 }
938 }
939 }
940 }
941 }
942 }
943 }
944 }
945 }
946 }
947 }
948 }
949 }
950 }
951 }
952 }
953 }
954 }
955 }
956 }
957 }
958 }
959 }
960 }
961 }
962 }
963 }
964 }
965 }
966 }
967 }
968 }
969 }
970 }
971 }
972 }
973 }
974 }
975 }
976 }
977 }
978 }
979 }
980 }
981 }
982 }
983 }
984 }
985 }
986 }
987 }
988 }
989 }
990 }
991 }
992 }
993 }
994 }
995 }
996 }
997 }
998 }
999 }
1000 }
```



# Define customData Value in Parameters File



The image displays two screenshots of a code editor window, showing JSON configuration files for FortiGate cloud-init parameters.

The top screenshot shows the file `C:\Users\gkaelin\Documents\Channel\Distributoren\ALSO\2018-10-24 FortiOS 6.0 Workshop - Azure\automation\parameters-fgt-cloudinit.json`. The JSON content is as follows:

```
13      },
14      "customData": {
15        "value": "Q29udGVudC1UeXB1OiBtdWx0aXBhcnQvbWl4ZWQ7IGJvdW5kYXJ5P
16      },
17      "FortiGateImageSKU": {
18        "value": "fortinet fg-vm"
19      },
20      "FortiGateImageVersion": {
21        "value": "6.0.3"
22      },
23      "instanceType": {
```

The bottom screenshot shows the file `C:\Users\gkaelin\Documents\Channel\Distributoren\ALSO\2018-10-24 FortiOS 6.0 Workshop - Azure\automation\parameters.json`. The JSON content is as follows:

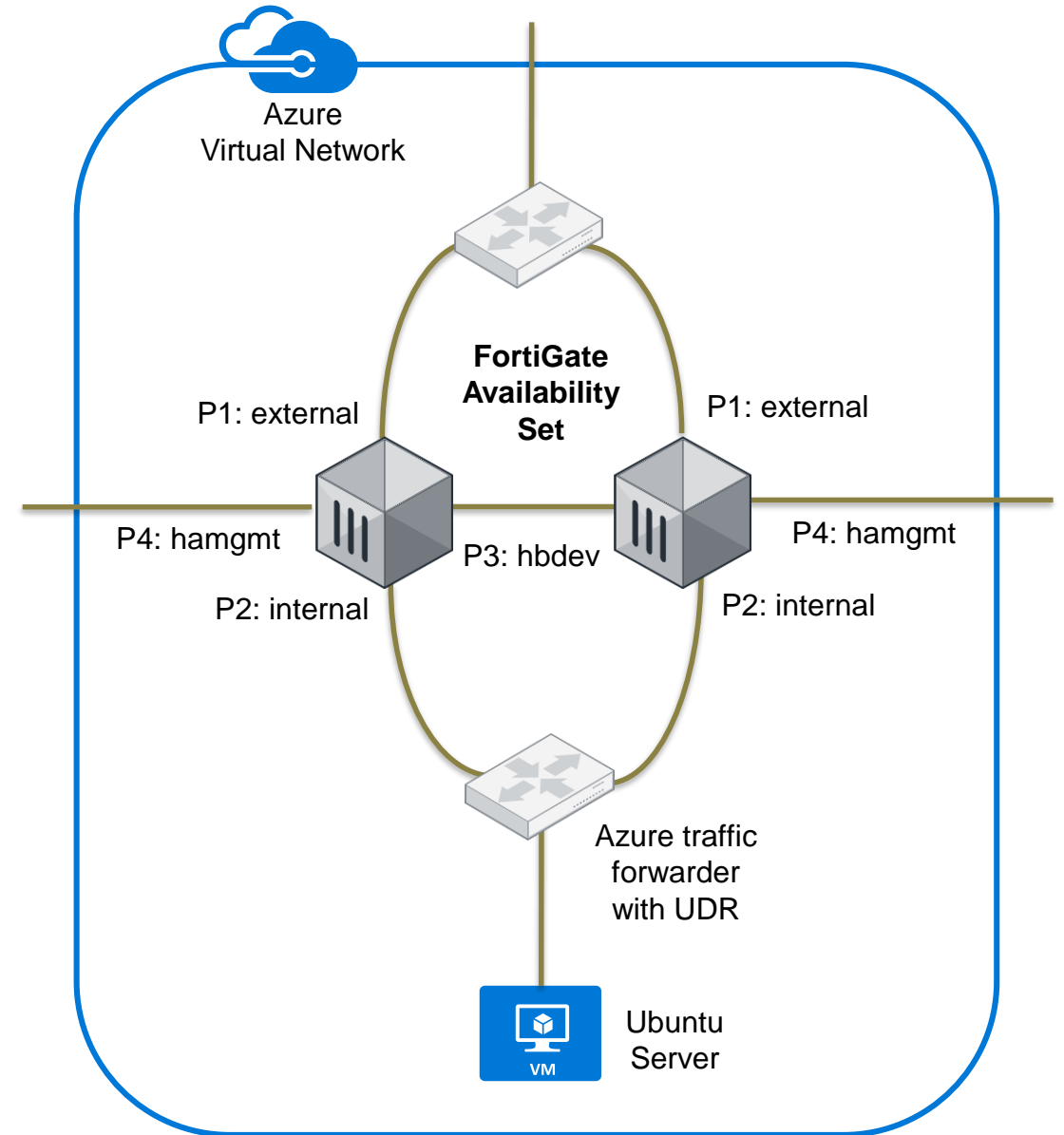
```
13      },
14      "FortiGateImageSKU": {
15        "value": "fortinet fg-vm payg"
16      },
```

Both screenshots show the editor's status bar at the bottom, indicating the file type as UNIX TXT and the current line and column numbers.

# Scenario 2: HA Active-Passive

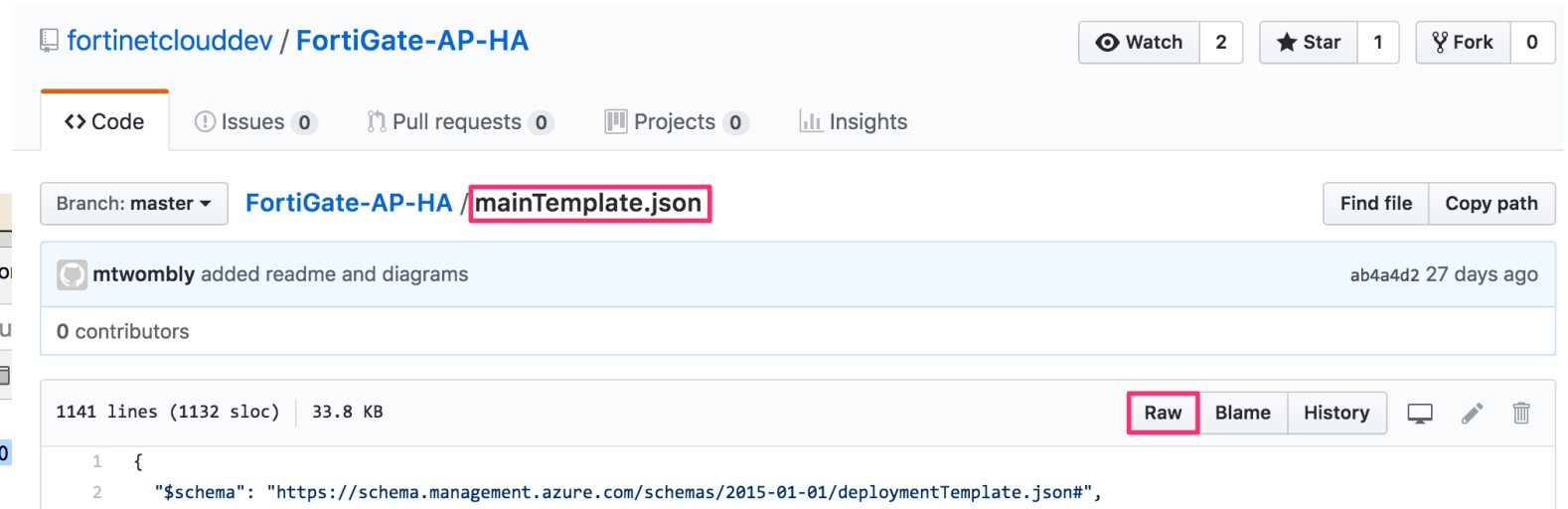
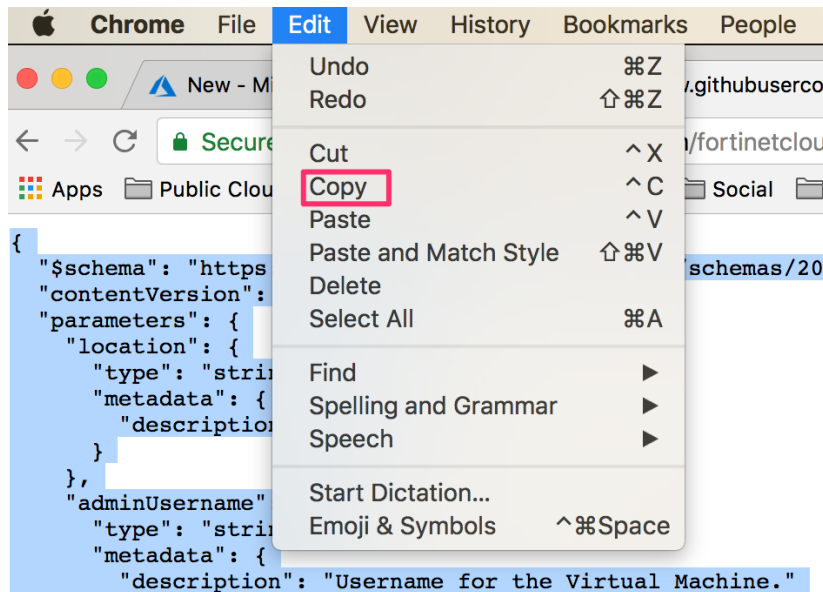
# New Active/Standby HA

- FortiOS 6.0.0 and 5.6.4
- Minimum three interfaces, better four
  - » Heartbeat and management interfaces in (hidden) sys VDOM, unusable for productive traffic
  - » Management interface for accessing firewalls
- Inside one Azure Region
- Additionally cloud-init support for Azure is now native to the cloud
- FortiGate VM for Azure also supports bootstrapping
  - » Will enable auto-scaling at some point



# Fetch latest FortiGate Template from GitHub

- <https://github.com/fortinetclouddev/FortiGate-AP-HA>
  - » Click 'MainTemplate.json'
  - » Click 'Raw'
  - » Select all and 'Copy'



# New HA CLI

- **HA Sync** must use unicast IP to sync, cannot use L2
- **Config sync** also now working over unicast IP addresses
- **Failover Mechanism** by sending commands directly to Azure
  - » Move public IP addresses
  - » Manipulate UDRs
- Failover times **unpredictable**
  - » Depends of number of items to re-write
  - » Serial change, not parallel

```
config system ha
    set group-name "Test"
    set mode a-p
    set hbdev "port3" 100
    set session-pickup enable
    set session-pickup-connectionless enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.1.3.1
        next
    end
    set override disable
    set priority 255
    set unicast-hb enable
    set unicast-hb-peerip 10.1.2.5
end
```

# Tips for Successful Failover Testing (1/2)

- Static IP addresses make sense
  - » Keep config in sync in Azure and FortiOS
- 'config system sdn-connector' files are not synced and require independent settings for NIC and UDR next-hop
- Inbound traffic requires two Virtual IP elements
  - » Firewall IP address config is not synced
- Remember static routes to internal networks
- Set override disable



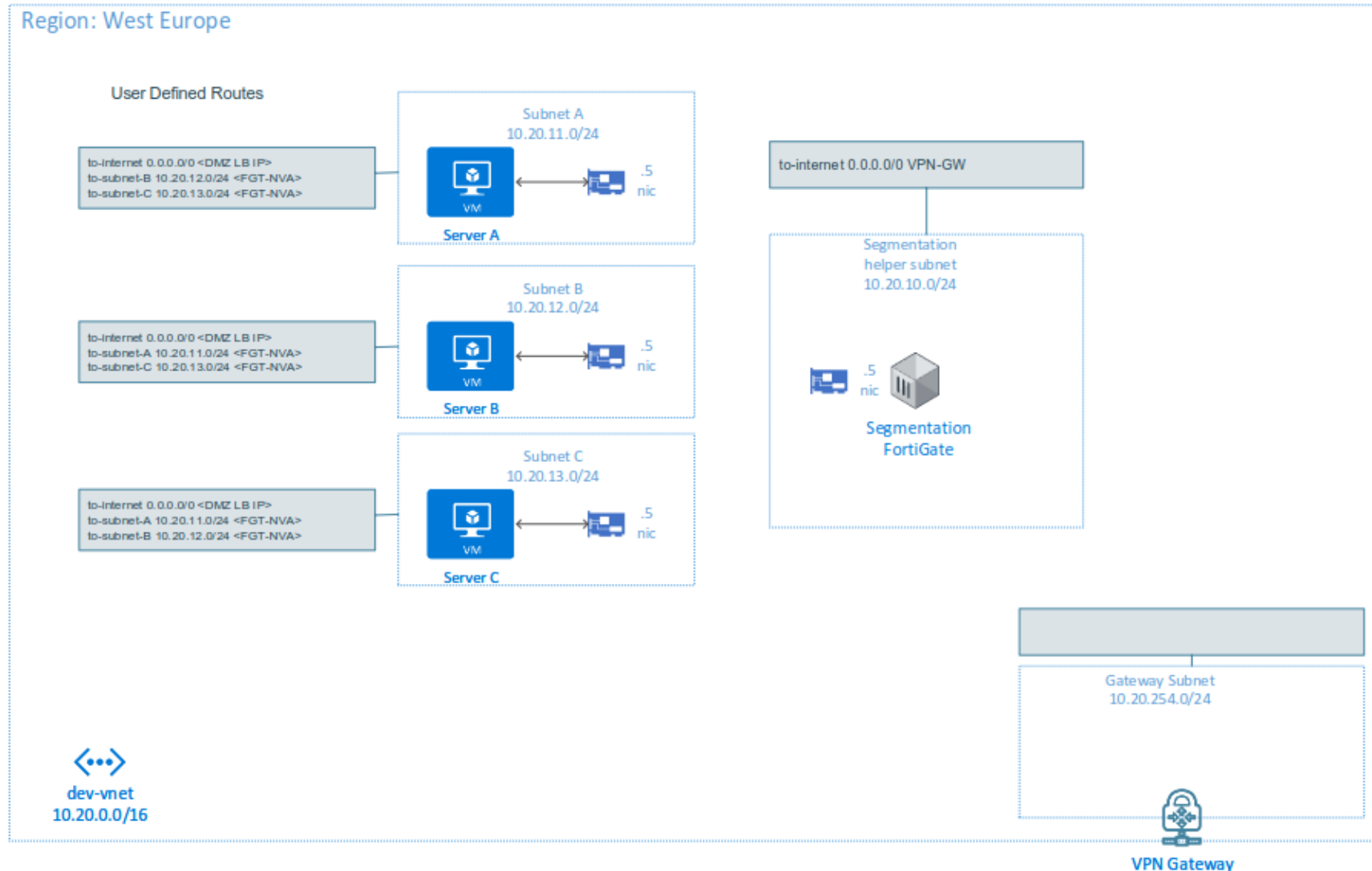
# Tips for Successful Failover Testing (2/2)

- diagnose sys ha checksum show
- diagnose debug application azd -99
- diagnose test application azd -1
  1. show HA stats
  2. SDN api test
  3. HA api test
  4. filter list test
  99. restart
- 'HA api test' is NOT a FGCP failover, leading to the twilight zone 😊
  - » Test with a real failure
- Make sure you have independent IP addresses. Remember, they are not synced ;)
- Headache with synced config, including node-specific IP addresses?

```
config system ha
    set sync-config disable
end
```

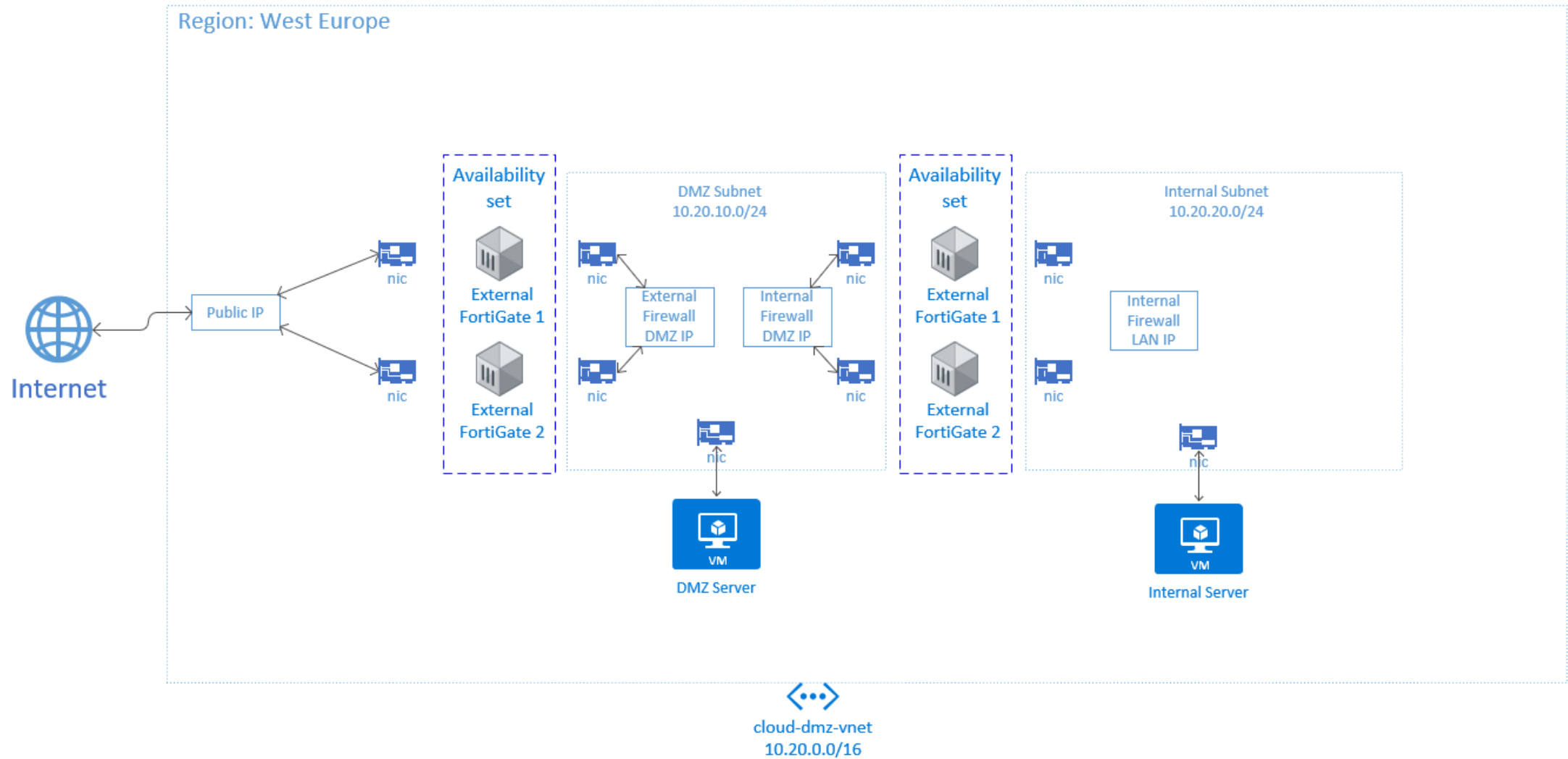
# Scenario 3: Network Segmentation

# Network Segmentation – Single Instance FortiGate

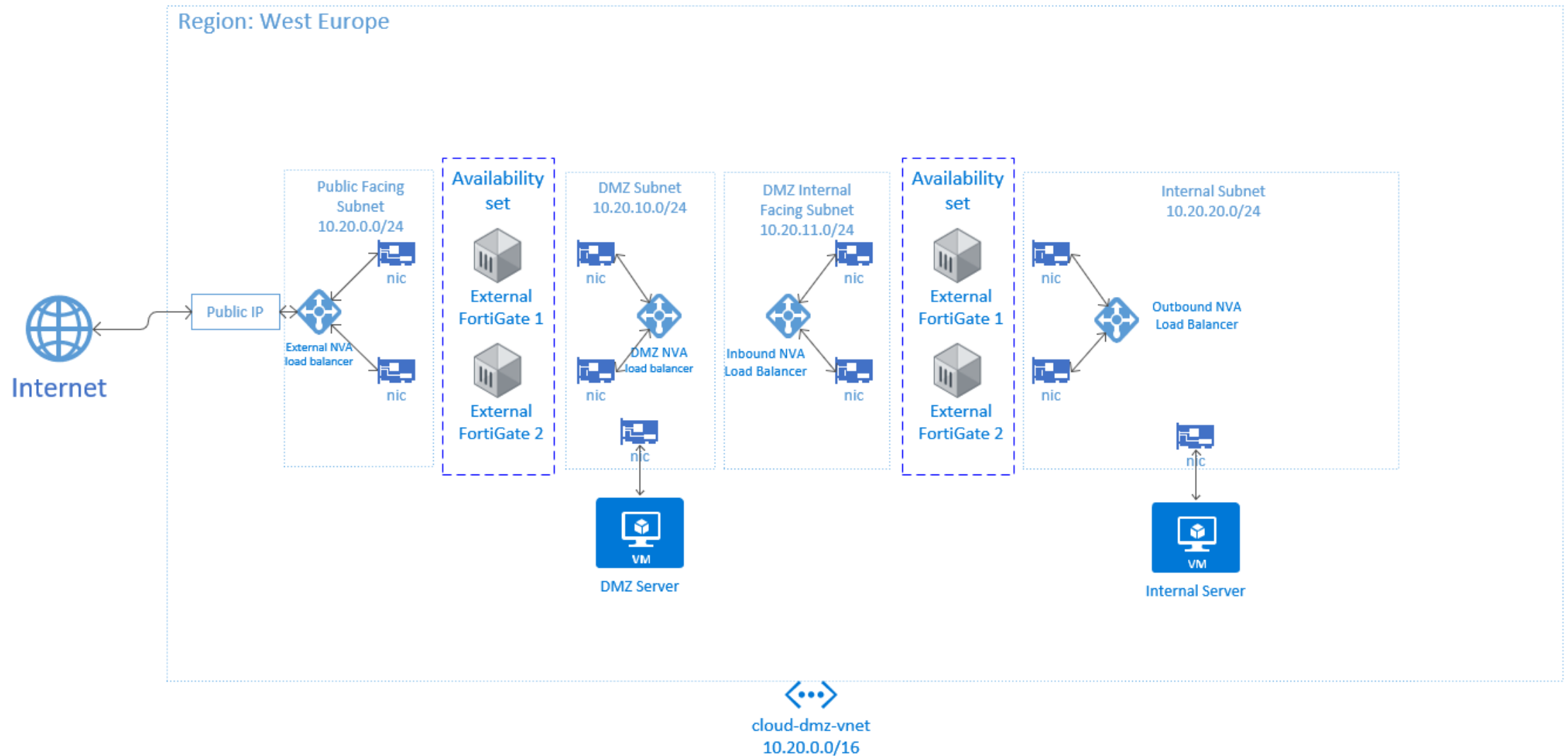


# Scenario 4: Cloud DMZ with HA Active-Active

# Wishful DMZ

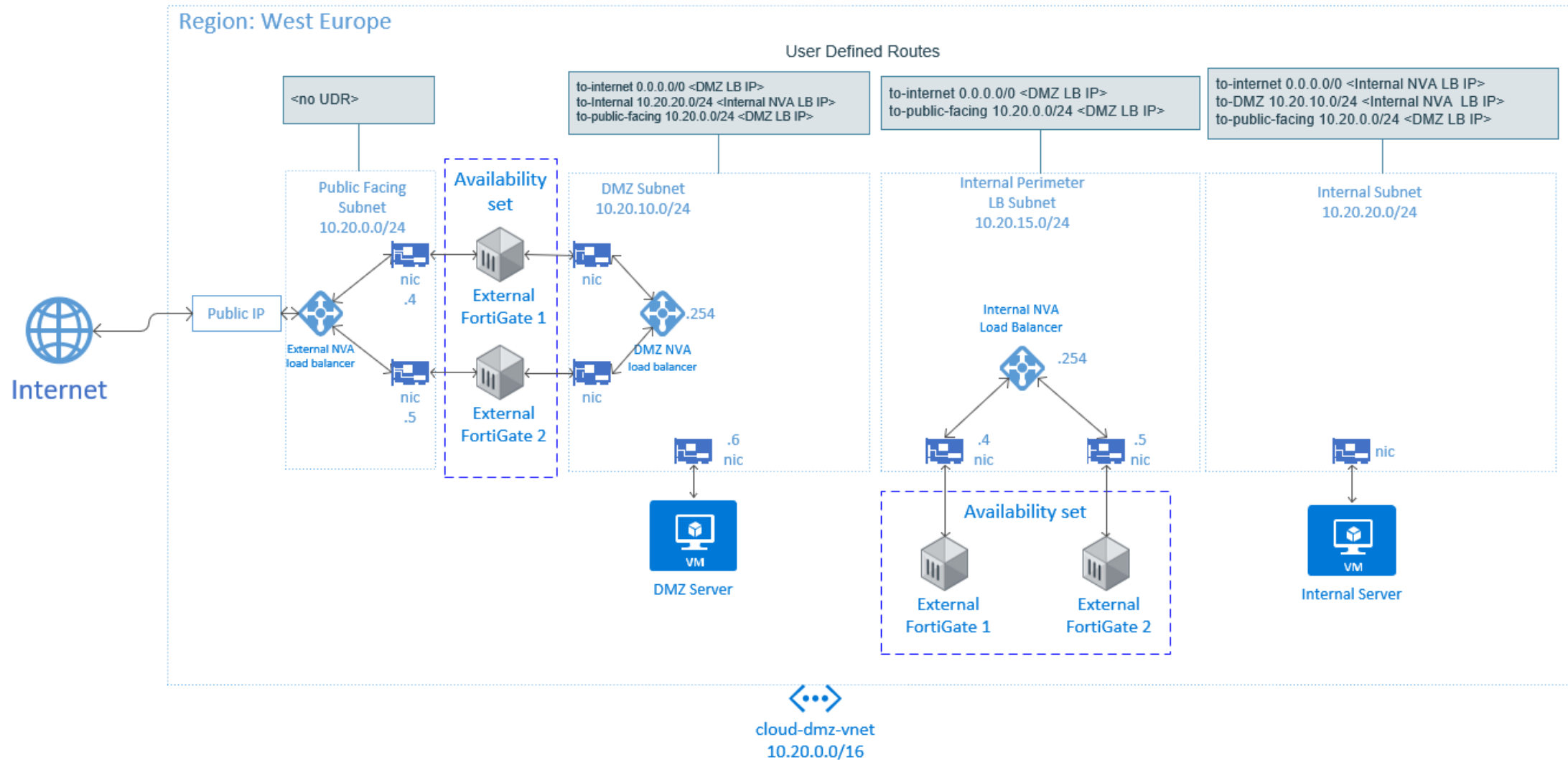


# One Step Towards Reality – Load Balancers Everywhere

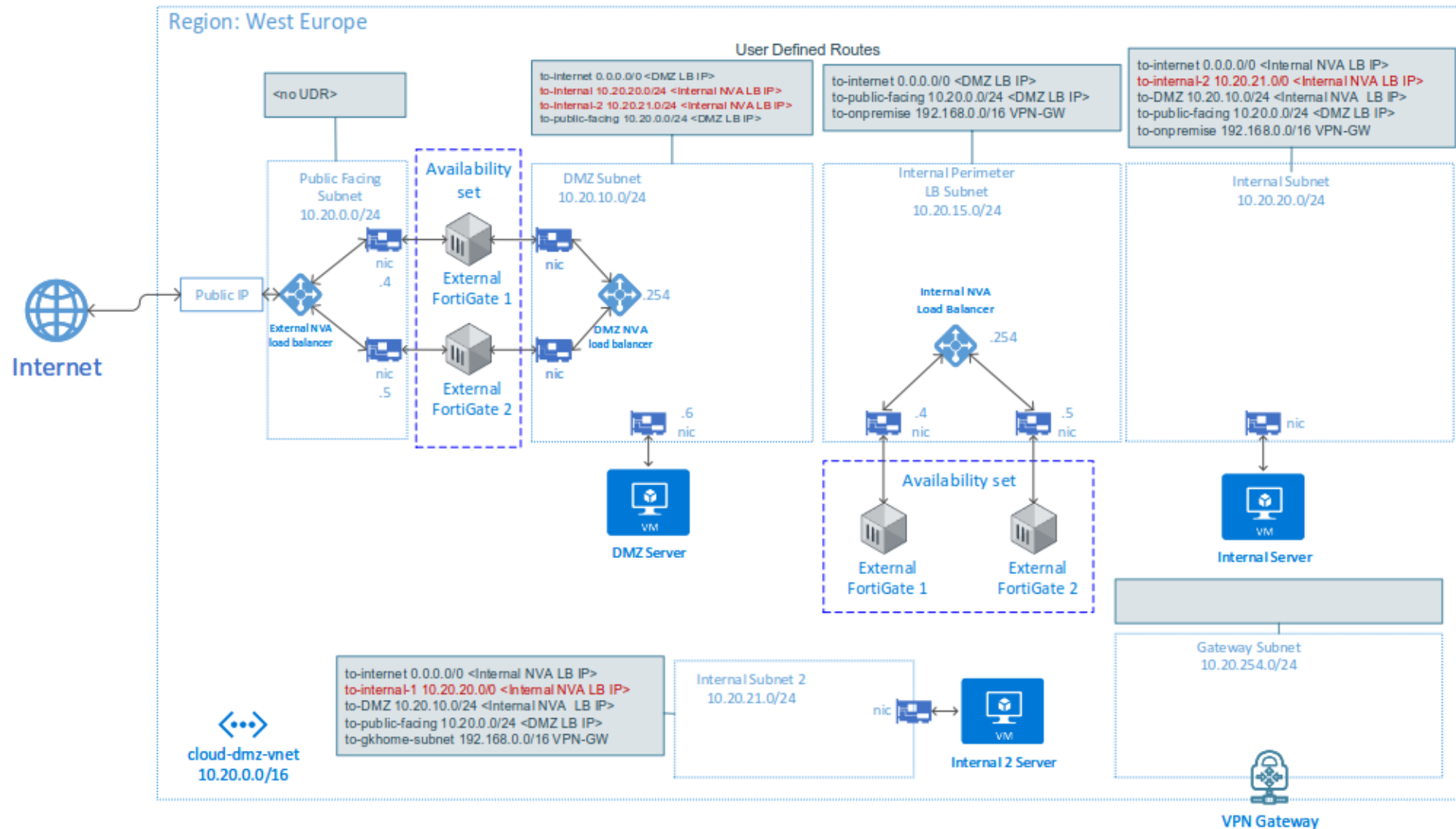




# Validated Design – Single Arm Internal FortiGate



# Cloud DMZ with Internal Segmentation



# External FortiGate Configuration – Routing

- There seems to be no way to check the backend probe status for Internal Load Balancers (Basic).
- Check probe traffic on FortiGate:

```
CldDmzFgtHaExt-A # diagnose sniffer packet port2 'port 22'
interfaces=[port2]
filters=[port 22]
2.441215 168.63.129.16.62861 -> 10.20.10.4.22: syn 1157932754
2.443124 168.63.129.16.62862 -> 10.20.10.4.22: syn 914950808
4.442631 168.63.129.16.62923 -> 10.20.10.4.22: syn 521302262
4.442654 168.63.129.16.62922 -> 10.20.10.4.22: syn 739689286
7.442191 168.63.129.16.62922 -> 10.20.10.4.22: syn 739689286
7.443232 168.63.129.16.62923 -> 10.20.10.4.22: syn 521302262
```

```
CldDmzFgtHaExt-A # diagnose sniffer packet port2 'port 22'
```

The screenshot shows the FortiGate VM64-Azure configuration interface. The left sidebar lists various configuration sections, with 'Static Routes' highlighted. The main area displays a table of static routes. A red arrow points to the second row of the table, which represents the route for the Azure Basic Internal Load Balancer's public IP address.

Destination	Gateway	Interface	Comment
10.20.10.0/24	10.20.10.1	dmz (port2)	
168.63.129.16/32	10.20.10.1	dmz (port2)	Azure - Internal Load Balancer ...

The Azure Basic Internal Load Balancer probes backend hosts for availability by using this public IP address!

# FortiGate Configuration – Session Sync with FGSP

## External FortiGate A

```
CldDmzFgtHaExt-A # show system cluster-sync
config system cluster-sync
    edit 1
        set peerip 10.20.10.5
        set syncvd "root"
    next
end

CldDmzFgtHaExt-A # show system ha
config system ha
    set hbdev "port2" 50
    set session-pickup enable
    set session-pickup-nat enable
    set override disable
end

CldDmzFgtHaExt-A #
```

## External FortiGate B

```
CldDmzFgtHaExt-B # show system cluster-sync
config system cluster-sync
    edit 1
        set peerip 10.20.10.4
        set syncvd "root"
    next
end

CldDmzFgtHaExt-B # show system ha
config system ha
    set hbdev "port2" 50
    set session-pickup enable
    set session-pickup-nat enable
    set override disable
end

CldDmzFgtHaExt-B #
```



# Create Internal FortiGate HA Cluster using Template

The image shows a sequence of three screenshots from the Microsoft Azure portal, illustrating the steps to create an internal FortiGate HA cluster using a template.

**Top Left Screenshot: Template deployment**  
The page title is "Template deployment". It explains that applications in Azure rely on resources like databases, servers, and web apps, and that Azure Resource Manager templates enable deploying and managing these resources as a group using a JSON description. It includes a "PUBLISHER" field set to "Microsoft".

**Top Right Screenshot: Custom deployment**  
The page title is "Custom deployment". It provides links to "Read the docs" and "Build your own template in the editor". A red arrow points to the "Build your own template in the editor" link.

**Bottom Screenshot: Edit template**  
The page title is "Edit template". It shows the "Load file" button in the top navigation bar, with a red arrow pointing to it. The main content area displays a JSON template for a FortiGate HA cluster. The template includes parameters for schema, content version, location, admin username, and admin password. The JSON is as follows:

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "location": {
6       "type": "string",
7       "metadata": {
8         "description": "location"
9       }
10    },
11    "adminUsername": {
12      "type": "string",
13      "metadata": {
14        "description": "Username for the Virtual Machine."
15      }
16    },
17    "adminPassword": {
18      "type": "securestring",
19      "metadata": {
20        "description": "Password for the Virtual Machine."
21      }
22    }
23  }
```



# Deployment Steps in this Demo

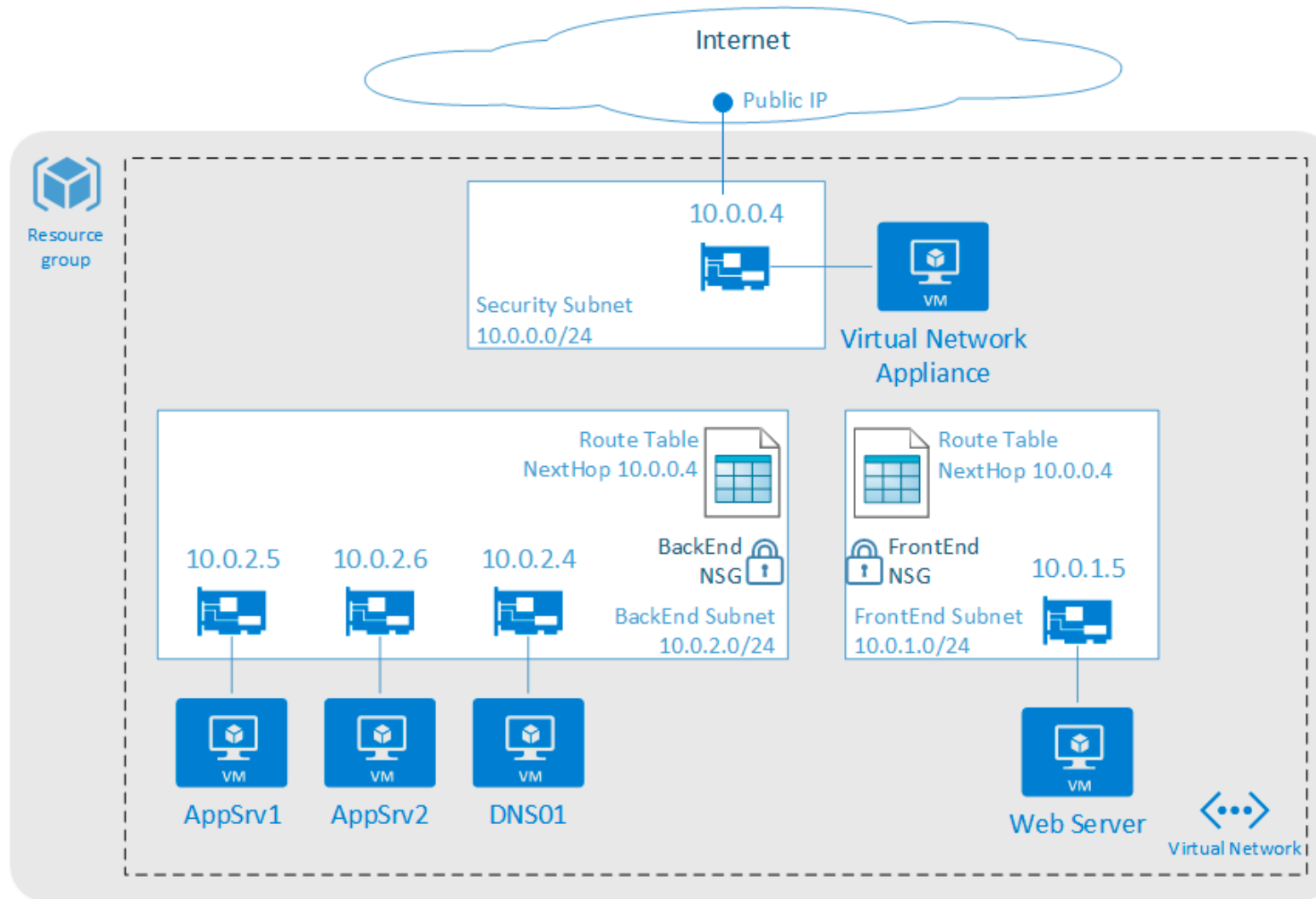
- Create Virtual Network and Subnets
- Deploy External FortiGate HA (A/A) Cluster from Azure Marketplace
- Configure External Load Balancer
- Configure external FortiGates
- Deploy DMZ Server
- Configure Azure load balancer and routes for outbound
- Deploy Internal FortiGate HA (A/A) Cluster from Template
- Configure internal FortiGates from DMZ Host
- Configure Azure internal load balancer and routes

# Lessons Learned

- Access internal FortiGates from DMZ server. I've encountered login difficulties when connecting from Internet – I wouldn't get past the login mask.
- Don't use ping to check connectivity to the Internet. It's not supported across Azure load balancers. Use e.g. Telnet instead.

# Wrap-Up

# Read Microsoft Documentation



<https://docs.microsoft.com/en-us/azure/best-practices-network-security>

# Glossary

- User Defined Routes

- » Policy routes which can override system and BGP routes on the Azure route service. These are typically required to engage FortiGate in an Azure VNET.

- Network Security Groups

- » Layer 3/Layer 4 ACLs which can be assigned to NICs or Subnets in Azure. These should not be configured on the same subnet with a UDR and a UDR route target (next hop), so typically not on the same subnet as the FortiGate.

- Availability Set

- » Provides a model to separate VMs into unique fault domains. This is the reliability model for Azure. FortiGates in HA should be in a common Availability Set

# Typical Technical Problems

## ■ Azure Routing

- » UDRs incorrectly deployed or not applied to appropriate subnet
- » UDRs and NSGs deployed on the same subnet as the FortiGate
- » UDRs not actually overriding system or BGP routes because they are not as specific

## ■ FortiGate Routing

- » FortiGate must have route to any network or subnet in which it doesn't have an interface.
- » FortiGate route table is distinct and disconnected from Azure routes.

The image features the FORTINET logo in white, bold, sans-serif capital letters. The logo is centered horizontally and slightly above the vertical center. The background is a solid red color. Overlaid on the red background are several faint, white, hexagonal outlines of varying sizes and orientations. Some of these hexagons are nested, creating a sense of depth. There are also some faint, white, circular outlines and lines scattered across the background, suggesting a network or molecular structure. The overall aesthetic is modern and technological.

**FORTINET®**